

Custom Security Intelligence

- Correlate an action(s) with a remediation (in this case, create a custom security intelligence block list)
- In this example we are looking for blocking events based on geolocation and dropping the source IP into the custom security intelligence list.
- Monitor the events in Firepower Manager for a match against a rule.
- The remediation runs a perl script on the Firepower Manager, which leverages the remediation framework to parse event information.

Custom Security Intelligence

Overview Analysis **Policies** Devices Objects AMP
Access Control ▾ Network Discovery Application Detectors Correlation **Actions ▶ Modules**

Installed Remediation Modules

Module Name	Version	Description
Blacklist IP	1.1	Add an IP Address to a feed used as a blacklist
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
ISE 1.2 Remediation	1.3.19	Quarantine IP addresses using Identity Services Engine 1.2
Nmap Remediation	2.0	Perform an Nmap Scan
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses
Set Attribute Value	1.0	Set an Attribute Value

Install a new module

No file selected.

Custom Security Intelligence

Policies | Devices | Objects | AMP

Network Discovery | Application Detectors | Correlation | **Actions ▶ Instances**

Edit Instance

Instance Name: Stop_Scanning
Module: Blacklist IP(v1.1)
Description:

Configured Remediations

Remediation Name	Remediation Type	Description
Bad_Host	Blacklist Source IP	<input type="text"/>

Add a new remediation of type:

Custom Security Intelligence

Policies | Devices | Objects | AMP

Network Discovery | Application Detectors | Correlation | **Actions ▶ Instances**

Edit Remediation

Remediation Name	Bad_Host
Remediation Type	Blacklist Source IP
Description	<input type="text"/>
File Name	<input type="text" value="scan.html"/>
MD5 File Name	<input type="text" value="scan_md5.html"/>
Restrict number of IPs in Blacklist?	<input checked="" type="radio"/> On <input type="radio"/> Off
IP host entry maximum	<input type="text" value="950"/>

Custom Security Intelligence

The screenshot shows a navigation menu with tabs: Overview, Analysis, **Policies**, Devices, Objects, and AMP. Below this, a secondary menu includes: Access Control ▾, Network Discovery, Application Detectors, **Correlation**, and Actions ▾. Under the 'Correlation' tab, there are sub-tabs: Policy Management, **Rule Management**, White List, and Traffic Profiles. The main content area displays a table with the following entries:

Name
<u>Unwanted Scan Traffic</u>
<u>Unwanted Scan Traffic - Repeat Offender</u>

Custom Security Intelligence

The screenshot displays the Cisco AMP web interface for configuring a custom security rule. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'Policies' section is active, with sub-tabs for 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions'. The 'Policy Management' section is selected, with sub-tabs for 'Policy Management', 'Rule Management', 'White List', and 'Traffic Profiles'. The 'Rule Information' section shows the rule name 'Unwanted Scan Traffic', an empty description, and the group 'Ungrouped'. There are buttons to 'Add Connection Tracker', 'Add User Qualification', and 'Add Host Profile Qualification'. The 'Select the type of event for this rule' section is set to 'If a connection event occurs at the beginning of the connection and it meets the following conditions:'. Below this, there are buttons to 'Add condition' and 'Add complex condition'. The conditions are listed as follows:

Operator	Field	Value
AND	Access Control Policy	is LISP Policy
	Device	is Virtual FirePower 10.0.0.102
	Source Country	is not United States
	Ingress Security Zone	is External
	Rule Action	is Block

The 'Rule Options' section includes a 'Snooze' field set to 0 hours and an 'Add Inactive Period' button. The 'Inactive Periods' section states: 'There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".'

Custom Security Intelligence

Select the type of event for this rule

If a connection event occurs at the beginning of the connection and it meets the following conditions:

AND

- Access Control Policy is LISP Policy
- Device is Virtual FirePower 10.0.0.102
- Source Country is not United States
- Ingress Security Zone is External
- Rule Action is Block



Custom Security Intelligence

Policy Management	Rule Management	White List	Traffic Profiles
Name			
<u>Bad Scanners</u> Watch for scanning from outside the US on vASA LISP IP			
<u>Repeat Offenders</u> Watch for scanning from outside the US on vASA LISP IP with multiple hits in X time (based on rule)			

Custom Security Intelligence

Overview Analysis **Policies** Devices Objects AMP Deploy 2 System Help **admin**

Access Control **Network Discovery** Application Detectors **Correlation** Actions

Alerts Remediations Groups

Policy Management Rule Management White List Traffic Profiles

Correlation Policy Information You have unsaved changes Save Cancel

Policy Name:

Policy Description:

Default Priority:

Policy Rules + Add Rules

Rule	Responses	Priority
<u>Unwanted Scan Traffic</u>	Bad_Host (Remediation)	Default 🔔 📄

Custom Security Intelligence

Responses for Unwanted Scan Traffic

Assigned Responses

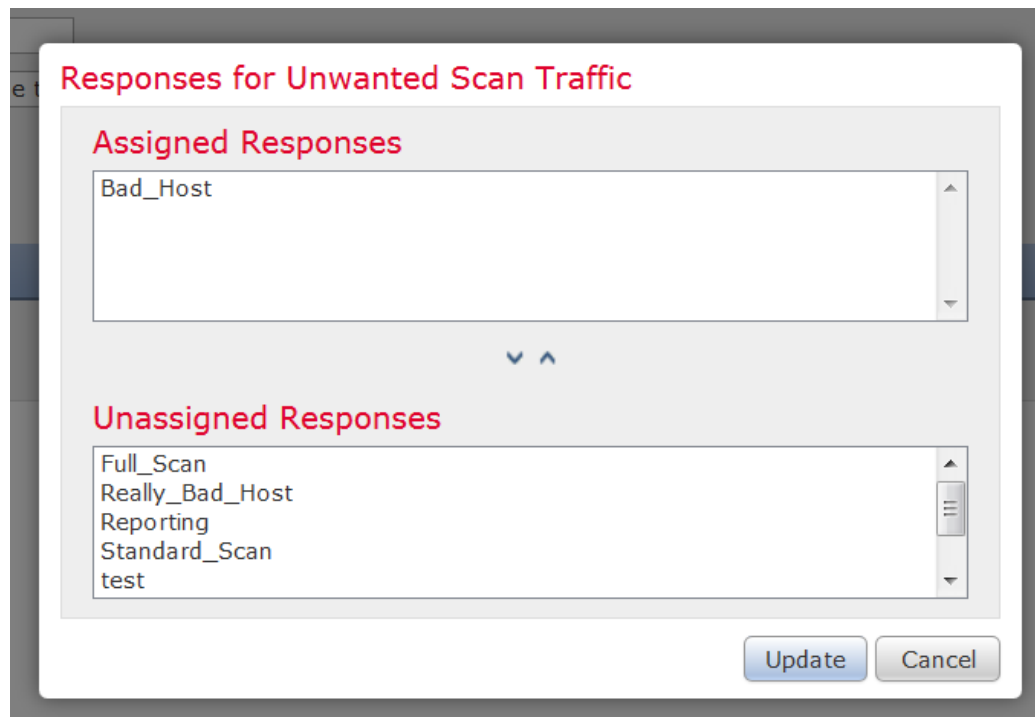
Bad_Host

▼ ▲

Unassigned Responses

Full_Scan
Really_Bad_Host
Reporting
Standard_Scan
test

Update Cancel



Custom Security Intelligence

Overview Analysis Policies Devices **Objects** AMP Deploy 2 Sys

Object Management Intrusion Rules

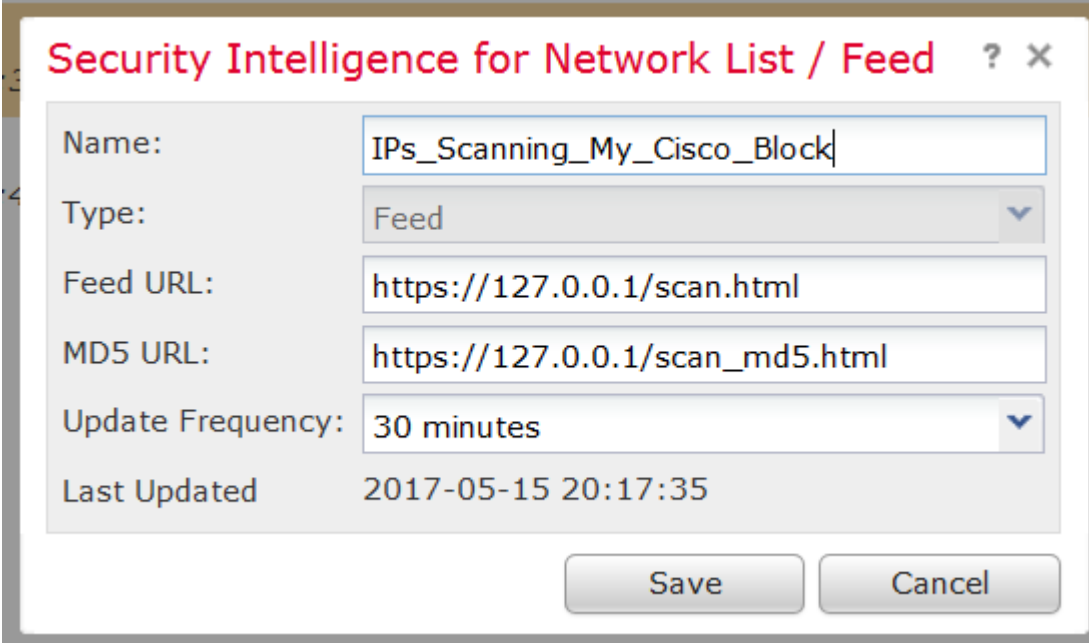
Update Feeds Add Network Lists and Feeds

Name	Type
Cisco-Intelligence-Feed <i>Last Updated: 2017-05-15 20:32:34</i>	Feed
Global-Blacklist	List
Global-Whitelist	List
IPs_Scanning_My_Cisco_Block <i>Last Updated: 2017-05-15 20:17:35</i>	Feed
test-list <i>Last Updated: 2017-02-08 16:54:45</i>	List

Network Lists and Feeds
DNS Lists and Feeds
URL Lists and Feeds



Custom Security Intelligence



The image shows a configuration dialog box titled "Security Intelligence for Network List / Feed". It contains several fields for configuring a security intelligence feed:

- Name:** A text input field containing "IPs_Scanning_My_Cisco_Block".
- Type:** A dropdown menu set to "Feed".
- Feed URL:** A text input field containing "https://127.0.0.1/scan.html".
- MD5 URL:** A text input field containing "https://127.0.0.1/scan_md5.html".
- Update Frequency:** A dropdown menu set to "30 minutes".
- Last Updated:** A text field showing the timestamp "2017-05-15 20:17:35".

At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

Reference Material

